

# Site Profiling

An Attackers  
View of Your Site

# Attacker's View

- Websites are a means to an end
  - Getting access to the server
- Content is irrelevant
  - TLD is a bonus however
- Dynamic is GOOD

# Who's out there

- The determined attacker will get in
  - Safest to assume this and plan for recovery
- The danger is the idle attackers
  - Script-Kiddies
  - Taggers
  - “Hacktivists”
- “Idiot Users”

# Script Kiddies

- Generic term
  - Popular since BBS'
- Unskilled attackers
  - Downloads a kit and runs it
  - Doesn't really know what it does
- A little knowledge ...
  - No telling what they'll do
  - Random fumbling

# Taggers

- Graffiti artists
- Moderately skilled
  - Usually watch vulnerability announces
  - Then they look for unpatched sites
- Bad press, high publicity
  - But low 'damage'
  - “Hacked by X-Kru”
  - Same process with Hacktivism

# Getting In

- Not usually manual
  - Scripts throw massive attack storms
    - Readily detectable by IDS
  - Programs scan for vectors
    - Linux/Apache doesn't need IIS attacks
  - Programs scan for known problems
    - Helps to narrow down the attack storm

# Defacement vs Attack

- Defacement is a high risk in .GOV
  - High profile, makes you look bad
  - Makes attacker look good
  - Graffiti on overpasses
- Attacks high in .COM, .MIL
  - Still a risk in all systems
    - Can be used to relaunch attack at .MIL
  - Tangible profit to attacker

# Profiling Programs

- Nessus
  - <http://nessus.org/>
  - Scans for known security problems
- NMAP
  - Scans for network configurations
  - <http://www.insecure.org/nmap/>
- Internet Security Scanner
  - <http://www.iss.net/>

# Fingerprints on the Silver

- All of the above leave log entries
  - Can detect attacks in progress
  - Can be used to detect attacks after-the-fact
  - Can identify attacker's profiling
    - Which might be usable to track the attacker!
- Logs bad
- Need to learn without leaving a scent

# Sniffing

- Network sniffing tells us a lot
  - Passive OS fingerprinting
  - TCP counters
  - Passwords !
- Still need to get inside the perimeter

# Sniffing Tools

- TCPDump and Ethereal
  - <http://www.tcpdump.org/>
  - <http://www.ethereal.org/>
  - Logs of traffic
  - Communication threads
  - Interpretable Data
- Everything we ever wanted to know!

# Touchless Car Wash

- Fingerprintless reconnaissance
  - Exploiting others reconnaissance
  - Not your fingerprints on the logs
- Various sites that have recon logs
  - But the original recon is still logged
  - Traceable (but complicated)
- Recon logs w/o recon
  - GOOGLE!

# Google Hacking

- Google Hacking Database
  - <http://johnny.ihackstuff.com/>
  - 1300+ Google searches
  - Symptomatic of security flaws
- Wikto
  - <http://www.sensepost.com/research/wikto/>
- Site Digger
  - [http://www.foundstone.com/resources/s3i\\_t](http://www.foundstone.com/resources/s3i_t)

# Tools

- Wikto & SiteDigger
  - Runs on Windows
  - .NET toolkit programs
  - Limited ability to restrict which searches
    - Last I looked, at least
- GHDB Scanner
  - Perl script
  - Range of restriction at category level
    - Still not that fine a resolution

# MSN Hacking

- Google Hacking is a generic term
  - Coke, Kleenex, etc
- Same technique works in any search
  - Even an internal search engine
  - Internal will index pages that only appear internally
    - The internal engine is inside the firewall
    - Can't view pages, but you get the contents!

# Anti Engine Options

- Robots files
  - Robots.txt tells engines where not to look
  - Which is a GREAT place to look
    - Indexing data is ignored by most IDS
- .htaccess
  - Slow annoying option
  - Put the directives in httpd.conf
    - Entry by Entry
    - “\*.int” ala .ht\* files

# Summary

- Need information for an attack
  - Looking yourself is dodgy
  - Reading others information is better
- Sources have identities
  - Whoevers logs your reading, they're known
  - Except auto-ignore entries
    - Like Search Engines!
- GHDB is a list of search terms
- Keep track of new vulnerabilities

# Summary

- Need information for an attack
  - Looking yourself is dodgy
  - Reading others information is better
- Sources have identities
  - Whoevers logs your reading, they're known
  - Except auto-ignore entries
    - Like Search Engines!
- GHDB is a list of search terms
- Keep track of new vulnerabilities

# Resources

- GHDB
  - <http://johnny.ihackstuff.com/>
- GHDB Scanners
  - <http://www.sensepost.com/research/wikto/>
  - <http://www.foundstone.com/resources/prod>
  - <http://climate.gsfc.nasa.gov/~dsinghal/secu>
- Open Source Vulnerability Database
  - <http://www.osvdb.org/>

# Questions?

- Dan Singhal
  - [dsinghal@climate.gsfc.nasa.gov](mailto:dsinghal@climate.gsfc.nasa.gov)
  - Email me if you have questions
- Presentation available at
  - <http://climate.gsfc.nasa.gov/~dsinghal/security/Profiling.pdf>